Duration: 3 Hours **Total Marks: 80**

N.B.: (1) Question No 1 is Compulsory.
(2) Attempt any three questions out of the remaining five.
(3) All questions carry equal marks.
(4) Assume suitable data, if required and state it clearly.

			Marks
Q1.		Attempt **any four**	
	a.	Describe Goals of Incident Response.	**5**
	b.	Define the term Digital Forensics and types of Digital Forensics.	**5**
	c.	Explain Social Engineering with example.	**5**
	d.	How to Present Digital Evidences?	**5**
	e.	Differentiate attack and vulnerabilities.	**5**
Q2.	a.	What is cybercrime? Explain the categories of cybercrime with example.	**10**
	b.	Differentiate between Computer worm, virus, Trojan horse and Trapdoor.	**10**
Q3.	a.	Draw and explain the Incidence Response Methodology in detail.	**10**
	b	List and explain the forensic image format with proper diagram.	**10**
Q4	a.	Discuss the necessity of forensic duplication and explain the use of dd, dcfldd, foremost, scapel command.	**10**
	b.	List and explain the steps involved in collecting volatile data in windows system.	**10**
Q5	a.	Case Study: A corporate lady was getting some threat mails. She decided to file a complaint. What steps should be taken to investigate those mails?	**10**
	b.	Explain with example CFAA act.	**10**
Q6	a.	Explain various types of laws and level of laws in details.	**10**
	b.	Write a short note on CAN Spam Act.	**10**